

REMARKS

This amendment and Request for Continued Examination is submitted in response to the Final Office Action mailed on October 17, 2007 and also in response to the Advisory Action mailed on February 11, 2008. Applicant thanks the Examiner for the further explanation of the rejection that is presented on page 3 of the Advisory Action. After carefully reviewing the Examiner's remarks, applicant has amended the claims to distinguish more clearly the prior art of record. Reconsideration and allowance of this application, as amended, is respectfully requested in view of the amendments and the remarks that follow.

The three independent claims 1, 17, and 22 are of similar scope – claim 1 is a method claim, while claims 17 and 22 are apparatus claims. Claim 22 differs from claim 17 in that it contains “means for” terminology. These three independent claims will be discussed together in the discussion which follows. Representative claim 1 will be the focus of the discussion below, which is also applicable to independent claims 17 and 22.

All of the claims stand rejected under 35 USC §103(a) as obvious in view of the combination of U.S. Published Application No. US 2002/0257267 A1 filed by John L. Williams, *et al.* on February 13, 2004 (claiming the priority of provisional application No. 60/448,313, filed on Feb. 14, 2003) with U.S. Patent No. US 6,229,540 B1 which issued to Daniel L. Tunelli, *et al.* on May 8, 2001. Reconsideration of this rejection is respectfully requested in view of this amendment.

In reviewing the comments of the Examiner presented in the Advisory Action dated February 11, 2008 and in the Final Rejection dated October 17, 2007, it appears clear to applicant that the Examiner's definition of the term “enterprise” is quite different from Applicant's proposed definition of that term. Applicant has pointed out to the Examiner a precise definition of the term “enterprise” that appears in paragraph [0030] of the specification, but the Examiner has declined to define the term “Enterprise” as that term is defined in the specification.

To briefly summarize the Examiner's position, the Examiner maintains that an "enterprise" is any collection of computers interconnected by a local area network and separated from the Internet (or separated from any wide-area network) by some form of protective firewall. Accordingly, the Examiner maintains that in Figure 1 of the Williams, *et al.* patent application (Pub. No. 2005/0257267 A1) discloses three separate enterprises of one business organization, one located in Chicago, another located in New York, and another located in London, since the Examiner notes that the computers and the interconnecting LANs 16 in each city are isolated from the Internet 18 by firewalls 24. (See the Examiner's statements presented on page 3, lines 1-9 of the February 11, 2008 Advisory Action and on page 5, lines 1-4 of the October 17, 2007 Final Rejection.)

To avoid any misunderstanding concerning the meaning of the term "enterprise," applicant in this amendment has amended the independent claims so that the preamble of each of the independent claims 1, 17, and 22 now includes a definition of the term "enterprise" that is taken from paragraph [0030] of the specification. In addition, a definition of the term "peer group," taken from paragraph [0046] of the specification, has been added as a final paragraph of each of these same independent claims. In addition, the claims have been further amended such that the term "node," which is defined in paragraph [0031] of the specification, has been replaced in all of the claims with the term "computer" to further clarify and simplify the claim language.

And to clarify that the enterprise presented in Figure 1 of the Williams, *et al.* patent application (Pub. No. 2005/0257267 A1) is a single enterprise that encompasses many or all of the computers of a single organization located in three cities, rather than three separate enterprises each defined by the isolation of computers behind firewalls as the Examiner has maintained, the term "enterprise" is defined in the claims as follows:

... the term enterprise is defined to be a collection of computers, software, and networking that interconnects the computing environment of an organization of people who may be widely distributed geographically,"

There is no mention of firewalls or cities or LANS versus WANS in this definition. If the computers are networked together and are used by people in a single organization, such as a company or a governmental organization or an educational institution or a hospital or the like, then the computers, their software, and the interconnecting network can form a single “enterprise” that may be audited for security.

The claims all require that security information be collected from the computers of a first “enterprise” which is being audited. This security information is analyzed to produce a first result of this analysis.

The claims next require this first result to be compared with a second result

comprising information derived from information previously obtained through application of the collecting and analyzing steps to one or more other enterprises that interconnect the computing environments of other different organizations of people who may also be widely distributed, these one or more enterprises together forming a relevant peer group of other different organizations of people, the result of this comparing step indicating the relative security of the first enterprise under audit relative to that of the peer group of one or more other enterprises;

The claims define a “peer group” to be

... a group of one or more enterprises assigned to the same business category as the first enterprise, enterprises involved in the same (or a similar) industry or business as the first enterprise, enterprises having computers configured similarly to the first enterprise’s computers, or enterprises required to comply with the same security standards as the first enterprise, or a combination of these.

The Examiner should note that the computers of the first enterprise under audit are not compared against any auditing standard – all such language has been deleted from the independent claims. The computers of the first enterprise are compared instead to the computers of other enterprises classified into the same “peer group” with the first enterprise. For example, the computers of one hospital are audited for security compliance, and the results of this audit are compared to the results of auditing for security compliance the computers of one or several other hospitals that form a peer group with the first hospital.

The specification states in paragraphs [0054] and [0055] some of the advantages of proceeding with a security audit in this way:

[0054] The reports generated following such a comparison focus upon the relative adequacy of the security measures in place within the enterprise being audited in comparison to the security norms in comparable enterprises, as is illustrated in Fig. 6, instead of focusing only upon the general security status of the enterprise. Accordingly, support engineers, and in particular engineers who may be skilled in enterprise security but not necessarily skilled in the security problems of the particular type of enterprise being audited (military, medical, academic, general business, etc.) do not have to wade through large amounts of security configuration information to identify and isolate problems – the security problems are highlighted by the comparative reports. Also, support engineers not necessarily skilled in the security aspects of enterprises in general do not have to concern themselves with failing to address some important security issue, since all relevant and material security issues are automatically addressed.

[0055] ... [A] report is generated that illustrates in detail the results of the comparison between the security configuration of the enterprise under audit and the ... industry averaged information for comparable industries (see, for example, the report 600 presented in Fig. 6). ...

The prior art Williams, *et al.* patent application (Pub. No. 2005/0257267 A1) does not work in this fashion. Williams, *et al.* compare the results of security auditing to standards, not to the results of auditing peer group enterprises. Accordingly, Williams, *et al.* does not teach the present invention as claimed.

Conclusion

The claims now before the Examiner are believed to be patentable over the art of record. Accordingly, their allowance is respectfully requested.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 08-2025. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 08-2025. If any extensions of time are needed for timely acceptance of papers

submitted herewith, Applicants hereby petition for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 08-2025.

Respectfully submitted,

Date February 19, 2008

By /James A. Sprowl/

FOLEY & LARDNER LLP
3000 K Street, NW
Washington, DC 20007
Telephone: 202-672-5399
(Attorney William T. Ellis)
Facsimile: 202-672-5399

James A. Sprowl
Attorney for Applicants
Registration No. 25,061
Telephone 847-446-7399